Ring, Field and Integraldomain

Chapter

TEN

NOTE

10.1 INTRODUCTION

After discussing group structure in a details in the last two chapters as the first algebraic structure being very important, we will survey briefly the other algebraic structures. Ring and Field and a particular form of ring structure known as integral domain in this chapter. These structures become easier to understand once the student becomes farmiliar with Group Structure because it will be present in every subsequent structure to be defined for study such new structure.

Group structure has been illustrated by taking examples from different types of sets just as set from number system, set of matrices etc and by taking one binary operation like addition all multiplication to test whether such a set satisfies the condition of group or not. Now in place of one binary operation, we will now consider two binary operations on these sets under certain specified conditions for such structures as range and field to see whether these sets satisfy those conditions or not to have such structures. One important thing one must notice that in the group structure whether we take sets from number system or from matrices etc. binary operations addition, and multiplication are ultimately provides the group structure under addition or under multiplication. So in our subsequent structures we will consider '+' and '.' as two binary operations to defne any general structures such as ring and field etc. But students should not think '+' and '.' as our ordinary addition and multiplication of number system but just a symbols for two binary operations to define such structures. These structures are required to the study of computer algebra, coding theory etc for computer system. Let us begin with ring structure defined as follows by taking symbol R for ring for any abitrary set under consideration just as symbol G was taken for Group.

10.2 RING STRUCTURE

Ring structure is another important algebraic structure. It consists of non-empty set R and two binary operation denoted by '+' and '$\cdot$' satisfying the following.

(a) $(R, +)$ is an abelian group.

(b) For any $a, b \in R$, $a \cdot b \in R$ that is R is closed under '$\cdot$' and R also satisfies the associative property under '$\cdot$' given by $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a, b, c \in R$.

(One can say that R is semigroup under '$\cdot$')

(c) '$\cdot$' Satisfies the distributive property over '+' from left and right given by for any $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{distribution from left} \qquad \ldots(1)$$

$$(b + c) \cdot a = b \cdot a + c \cdot a \qquad \text{distribution from right} \qquad \ldots(2)$$

Then R is called ring denoted by $(R, +, \cdot)$.

From the definition of ring one can see that group is there to define ring structure. Just as if any non-empty set X is to be tasted for ring under binary operation '+' and '$\cdot$' one has to test the set X that (i) it must satisfy all the five property of abelian group and it must be semigroup, under '$\cdot$' that is it is closed and associative. Since '$\cdot$' may not be commutative so in (c) one has to test the distributive property of '$\cdot$' over '+' both from left as well as from right. Thus in a nut shell for any set X to be ring R it must satisfy 9 properties, five for abelian group under '+' and two for semigroup under '$\cdot$' and two for distributive properly from left and right so as to qualify for ring structure.

NOTE

10.2.1. Different form a Ring : Before we give examples on ring as we did in group structure, we will first consider different form of ring that will be required in the examples as well as in the study of other properties of ring. However one simple example that one must see is the set of integers. $I = [0, \pm 1, \pm 2, \pm 3, \ldots]$ which has been shown as an example in group theory that $(I, +)$ is an a abelian and $(I, \cdot)$ is commutative semi group with identity element '1' as monoid is the first ring structure under number system and a very important ring structure for various other form of ring to be discussed below.

10.2.2. Commutative ring : The ring $(R, +, \cdot)$ is called commutative ring if R satisfies the commutative property under '$\cdot$' that is, $a \cdot b = b \cdot a \ \forall \ a, b \in R$

The obvious example is again $(I, +, \cdot)$ which is commutative semi group under '$\cdot$'.

10.2.3. Ring with Unity : Any ring $(R, +, \cdot)$ is said to be ring with unity if R has identity element usually denoted by '1' under second binary operation '$\cdot$'.

Again $(I, +, \cdot)$ is a ring with unity as $1 \in I$ is identity element for multiplication under I.

10.2.4. Commutative Ring With Unity : Any Ring $(R, +, \cdot)$ is said to be commutative ring with unity if R satisfies both 10–2.2 and 10.2.3 under '$\cdot$', that is, R is both comutative and has identity element under '$\cdot$'.

$(I, +, \cdot)$ is an example of commutative ring with unity.

10.2.5. Ring without zero divisor : Any ring$(R, +, \cdot)$ is called ring without zero divisor if for any $a, b \in R \quad a \cdot b = 0 \Rightarrow$ either $a = 0$ or $b = 0$ where '0' is identity element of R under '+'.

10.2.6. Ring with zero divisors : Any ring $(R, +, \cdot)$ is said to be ring with zero divisor if for any $a, b \in R$

$$a \neq 0 \text{ and } b \neq 0 \Rightarrow \quad a \cdot b = 0$$

The students should rote that example of ring without zero divisor of 10.2.5 is again $(I, +, \cdot)$ or any number system under '$\cdot$'from ordinary algebra where we always say $xy = 0 \Rightarrow$ either $x = 0$ or $y = 0$ but number system does not satisfies 10.2.6.- Ring with zero divisor. This example will be found in matrices where there are matrices which are not zero but their product is zero. Just as if we consider $A = \begin{bmatrix} 1 & 1 \\ 4 & 4 \end{bmatrix} B = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$ as 2×2 matrix where $A \neq 0, B \neq 0$

But $AB = \begin{bmatrix} 1+(-1) & (-1+1) \\ 4+(-4) & (-4+4) \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$

Thus the set of matrices which is ring under matrix addition and multiplication (see example from group theory on matrices) is ring with zero divisor.

10.2.7. Integral domain : It is a particular form of ring where any ring $(R, +, \cdot)$ is a commutative ring with unity without zero divisor is called an integral domain.

Again one can see $(I, +, \cdot)$ is an example of Integral domain.

Remark : Some authors define integral domain as commutative ring without zero divisor and do not include identity element 'unity' under '$\cdot$' to define integral domain.

10.2.8. Field : Now we define another important structure field from ring structure as follows. Any commutative ring with unity $(R, +, \cdot)$ is said to be field if non-zero element of R, that is all element of R other than identity element '0' under '+' has its inverse under '$\cdot$', that is for each $a \in R \Rightarrow a^{-1} \in R \ a \neq 0$

Then $(R, +, \cdot)$ is expressed $(F, +, \cdot)$ replacing symbol R for ring by symbol F for Field.

NOTE

10.2.9. General definition of Field : In general field is defined like group ring from non-empty set as follows.

Any non empty set F under two binany aperations denoted by '+' and '$\cdot$' is said to be field if F satisfies the following.

(a) $(F, +)$ is an abelian group.

(b) $(F/0, \cdot)$ is an abelian group, that all element of F other than '0' as identity element '+' is again abelian group under '$\cdot$'.

(c) Since '$\cdot$' is commutative so the distributive property of '$\cdot$' over '+' does not required left or right distributive condition and simplify say '$\cdot$' satisfies the distributive property of '$\cdot$' over '+' that is, for any $a, b, c \in F \quad a \cdot (b + c) = a \cdot b + a \cdot c$

Example of field

Thus for any set 'X' to be qualified for field it must satisfies 5 properties of abelian group each under '+' as well as under '$\cdot$' that is 10 properties and one property as distributive property of '$\cdot$' over '+'. Thus in total it must satisfy eleven properties to become field F. Now if consider example examples on infinite groups under number system then one can see that the set of rational number Q, set of real number R and set of complex number C be checked for '+' and '$\cdot$' binary operation and when R, C are taken non-element for under '$\cdot$' they are abelion group both '+' as well as under '$\cdot$' Moreover we also know from algebra that all such number system satisfy the distributive property of multiplication over addition but does not satisfy the distributive property of addition over multiplication. Hence $(Q, +, \cdot), (R, +, \cdot)$ and $(C, +, \cdot)$ are the obvious examples of infinite field.

Again since commutative ring with unity is condition to satisfied by field so as per definition 10.1.10 one can say $(Q, +, \cdot), (R, +, \cdot)$ and $(C, +, \cdot)$ are also all commutative ring with unity as well. Moreover, since we also know that in algebra that $xy = 0 \Rightarrow x = 0$ or $y = 0$ holds. So $(R, +, \cdot)$ and $(C, +, \cdot)$ are the examples of ring without zero divisor moreover, they are all also Integral domain. Hence one can say that every field is an integral domain but converse is not true as $(I, +, \cdot)$ is also integral domain but $(I, +, \cdot)$ is not a field.

10.2.10. Division Ring (Skew field) : Now we derive another structure known as Division ring (also called as Skew field), that is when ring $(R, +, \cdot)$ with unity is such that its non-zero element has its inverse under '$\cdot$' called as every element of R is invertible then $(R, +, \cdot)$ is called Division ring or Skew field denoted by $(D, +, .)$

Example of Division Ring : Now Division ring differs from field in the sense that it is not commutative under '$\cdot$' as required for F. So it is called skew field.

The example of skew field is the set of matrices. In general set of square matrices M given by $M = \{A = A = (a_{ij})_{n \times n}\}$ under '+' and '$\cdot$' is Ring with unity, because if one checks the examples on matrices under group theory, then one will see that $(M, +)$ is an abelian group and $(M, \cdot)$ is non commutative semi group with Identity matrix as Identity element under the product of matrices and but when the set of square matrices becomes a set of non-singular square matrices then every such matrix has its inverse defined as every matrix is invertible so such a non singular set of square matrices under '+' and '$\cdot$' is example of Division ring or Skew field.

10.2.11. Boolean Ring : If any ring $(R, +, \cdot)$ satisfy the Idempotant property under '$\cdot$' that is, $a \cdot a = a \Rightarrow a^2 = a$. Then any such ring $(R, +, \cdot)$ is called Boolean Ring.

NOTE

10.3 EXAMPLES OF RINGS

Though we have discussed many examples on various types of rings, bet we will summarize them for the benefit of students to remember them.

10.3.1. (1) Example of Infinite Ring

(a) Number system

(i) $(I, +, \cdot)$ commutative ring with unity 1 without zero divisor. Integral domain but not field.

(ii) $(Q, +, \cdot)$ an integral domain as well as field.

(iii) $(R, +, \cdot)$ An integral domain as well as field.

(iv) $(C, +, \cdot)$ integral domain as well as field.

(b) Soft of Matrix

(i) $M = \{A = A = (a_{ij})_{m \times n}\}$ be set of $m \times n$ matrices then $(M, +, \cdot)$ is only ring but neither commutative ring nor ring with unity but it will be a ring with zero divisor, so it is not integral domain.

(ii) $M = \{A = A = (a_{ij})_{n \times m}\}$ be set of square matirces then $(M, +, \cdot)$ is a ring with unity but not commutative as ring with zero divisor. It is not integral domain.

(iii) $M = \{A = A = (a_{ij})_{n \times m}\}$ be set of non-singular square matrices. Then it becomes Division Ring (Skewing fields) but not field. So it is not an integral domain.

(c) Set of Real Valued Function :

Let $A = \{f : f : R \to R\}$ be the set of real valued function defined on R to R. Let two binary '+' and '$\cdot$' be defined as addition of function and '$\cdot$' as composition of mapping given by

(i) $(f + g)(x) = f(x) + g(x) \; \forall \; x \in R$

(ii) $(gf)(x) = g(f(x)) \; \forall \; x \in R$

then $(A, +;)$ is ring with unity.

Solution. To prove it we have to show that

(a) $(A, +)$ is an abelian group.

(b) $(A, \cdot)$ is semi group as well as Monoid

(c) '$\cdot$' is distributive over '+'.

To prove (a) that $(A, +)$ is an abelian group it must satisfy G-1 to G-5 properties.

G-1: since for any $x \in R$, the binary operation '+' as defined by (i) is given by

$$(f + g)(x) = f(x) + g(x)$$

Since $f(x), g(x) \in R \Rightarrow f(x) + g(x) \in R \quad \forall \; x \in R \Rightarrow (f + g)(x) \in R \quad \forall \in R$

$\Rightarrow (f + g) \in A \;\; (G - 1)$ condition of group holds.

G-5 : Moreover, $f(x) + g(x) = g(x) + f(x) \forall \; x \in R$ as real number are commutative under '+'.

$\Rightarrow (f + g)x = (g + f)(x)$

$\Rightarrow f + g = g + f$ Hence $(G - 5)$ holds of group under '+'. So A is commutative under '+'.

G-2 : Since real number under '+' satisfy the associative property given by $(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x)) \quad \forall x \in R$. So for any $f, g, h \in A$

$\Rightarrow \; (f + g) + h = g + (g + h)$

Hence $(G - 2)$ condition holds in A under '+'.

G -3 Existence identity : We define zero map as denoted by $\hat{0}$ and express it as $\hat{0}(x) = 0 \; \forall \; x \in R$

Then $\hat{0}$ will be identity element for '+' in A. To prove it we have by definition of '+' in (i)

$$(f+\hat{0})(x) = f(x)+\hat{0}(x)$$
$$= f(x)+0 \qquad \text{By definition of } \hat{0}$$
$$= f(x)$$
$$= \hat{0}(x)+f(x) = (\hat{0}+f)(x) \forall\ x \in R$$

Hence $f+\hat{0} = f = \hat{0}+f\ \forall\ x \in R$ so $G-3$ condition holds.

G - 4 Existence of Inverse : Since we know for any real number $a \in R\ \exists -a \in R$ such $a+(-a) = 0 = -a+a$ So taking $a = f(x) \in R \Rightarrow -f(x) \in R$

$$\Rightarrow \qquad f(x)+(-f(x)) = 0 = -f(x)+f(x)$$

$$\Rightarrow \qquad f(x)+(-f(x)) = \hat{0}(x) = -f(x)+f(x) \qquad \text{By definition of } \hat{0}$$

$$\Rightarrow \qquad (f+(-f))(x) = \hat{0}(x) = (-f+f)(x) \forall\ x \in R$$

$$\Rightarrow \qquad f+(-f) = \hat{0} = -f+f$$

Hence for every $f \in R - f \in A$ as additive inverse, satisfying the $G-4$ condition. Thus $(A, +)$ becomes a abelian group. Hence (a) condition holds.

(b) To prove (b) we must show that $(A,\cdot)$ under the definition given by (ii) is closed and associated and has identity element '$\cdot$'. Now as per definition given by (ii) we have $(gf)(x) = g(f(x)) \forall\ x \in R$ Since by definition $f(x) \in R \Rightarrow g(f(x)) \in R \Rightarrow (gf)(x) \in R$. So $gf \in A$ hence A is closed under '$\cdot$'. Moreover, under the composition of mapping in example under group theory that composition mapping is not always commutative but is always associative. Therefore A will satisfy associative property under '$\cdot$' thus A will be semi group under '$\cdot$' again we know that Identity mapping I is an Identity element under the '$\cdot$' composition mapping given by $fI = f = If$

So $(A, \cdot)$ is semi group with unity.Hence $(A, \cdot)$ is a monoid.

(c) Distributive Property : Again we know in real number the multipliction satisfies distributive over '+' given by a $(b+c) = ab+ac$ for $a, b, c \in R$. So taking a, b, c as f, g, h we have

$$(f(g+h))x = f(g(x)+h(x)) \qquad \text{By definition of composition mapping} \qquad \ldots(1)$$
$$= f(b+c) \qquad \text{Taking } g(x) = b\ h(x) = c \qquad \ldots(2)$$
$$= f(b)+f(c) \qquad \text{By definition of '+' by (i) for } A \qquad \ldots(3)$$
$$= fg(x)+fh(x)$$

$$\Rightarrow \qquad f(g+h)x = (fg+fh)(x) \qquad \text{By definition (ii)} \qquad \ldots(4)$$

$$\Rightarrow \qquad f(g+h) = fg+fh \quad \forall x \in R \qquad \ldots(5)$$

Thus $(A, \cdot)$ is a ring with unity.

However if, one take $A = \{f : f : R \to R\}$ as a set of bijective mapping then each f will have unique inverse and under the composition of mapping it will satisfy $ff^{-1} = I = f^{-1}f$

Then A will becomes Division ring.

10.3.2. Example of Finite Ring/Field : We have discussed some important examples of infinite rings from the example on infinite groups. Now we will discuss some important example of finite ring as well as of field.

NOTE

NOTE

If one checks all the examples discussed on finite groups one will find that only modulo groups become qualify to consider for finite ring the other finite groups cannot be considered why? The answer is that no other finite group is formed under two separate binary operation. All other finite groups are groups under one binary operation as multiplication.

(i) Example from modulo system : We have consider modulo system for groups under modulo addition as well as modulo multiplication. (see example 4, 5 as under 8.3.4 and its extension 8.3.5.) It has been explained in example 4, 5 and by 8.3.5 that $a \cong b \bmod m$ where m is any positive integer and $a, b \in I$ where $I = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$ as set of integers then there is a set of m residue classes under modulo m expressed as $I / \bmod m = \{[0], [1], [2], \ldots, [m-1]\}$

But when m is a prime number p then under modulo addition as well as modulo multiplication it will have abelian groups see examples 4 and 5 where for $m = 5$ it is abelian group under modulo multiplication when we take only non zero residue classes.

Thus for $m = p$ where p is prime we have $I / \bmod p = \{[0], [1], [2], \ldots, [p-1]\}$ …(1)

is a abelian under modulo addition defined as $[a]_p + [b]_p = [a+b]_p$ …(2)

and $G = \{[1], [2], \ldots [p-1]\}$ as a non zero modulo classes under modulo p …(3)

is again abelian groups under modulo multiplication defined as $[a]_p [b]_p = [ab]_p$ …(4)

Moreover modulo group under multiplication for non zero classes for prime number has identity element [1] as well as. Thus one can say $(I \bmod p, +, \cdot)$ is a field under modulo addition and modulo multiplication expressed as $(I \bmod p, +, \cdot)$

Since it is field so it is also commutative ring with unity.

Since it is a field so it is also Integral domain.

(ii) However, when m is not prime number, let $m = 6$ then it has been explained in 8.3.5 that it is an abelian groups under modulo addition but its non zero classes is not a group under modulo multiplication as it fails to be closed. So it is not a field. But we will show that it is commutative ring with zero divisor by constructing composition tables taken for $m = 6$ under modulo addition and multiplication as shown below.

Composition Table for modulo 6 under Addition

$+_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Table - 12

One can easily check that it is an abelian group under modulo addition so $(I / \bmod, +)$ satisfies the condition of ring under '+'. For modulo multiplication we will consider some set of classes not non zero classes, because we have to prove that under modulo multiplication it is commutative semi group not field.

NOTE

Composition Table for modulo 6 under Multiplication

$\cdot_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Table - 13

From multiplication table you can check that it is closed. So $G-1$ condition holds.

For $G-2$ condition one has to check that it is associative. Now to verify it let us consider any set of three number say $a=[2], b=[3], c=[5]$ then to test that $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ holds …(1)

Now let us consider LHS of (1) expressed as $([a]\cdot[b])\cdot[c]$ on taking the value of a, b, c it becomes $(a\cdot b)\cdot[c]=([2][3])[5]=[6][5]=[0][5]=[0]$ (See table - 13) Again let us consider RHS of (1) we have $a\cdot(b\cdot c)=[2]\cdot([3]\cdot[5])=([2][15]_6)=[2][3]=[6]=[0]$ (as per table-13)

Thus $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ of (1) holds. It can be checked for any three numbers from set, thereby proving that it satisfies the associative property so G_2- condition holds.

Hence $(I \text{ / mod } 6)$ is a semi group.

G -5 condition : To check that it is commutative as well, let us, again consider any pair of number say as [4] and [5] and one can see that $[4][5]=[20]_6=[2]=[20]_6=[5]\cdot[4]$ as per Table- 13. Similarly one can see that $[3]_6\ [5]_6=[3]=[5]_6\ [3]_6$

Thus $(I \text{ / mod}_6, \cdot)$ is a commutative semi group.

Distributive Property : Lastly one can easily check that it satisfies the distributive property of multiplication over addition. Since it is commutative semi group under multiplication, so left (right) distributive property condition will not be required. Just distributive property in any form will serve the purpose. So let us take $a=[2],[b]=3,[c]=5$ and test for

$$[2]([3]+[5])=[2][3]+[2][5] \quad \ldots(2)$$

Now to verify it one can see from table of addition and multiplication that LHS of (2) will be given by $[2]([3]+[5])=[2][8]_6=[2][2]=[4]$ again let us consider RHS of (2) then we have

$[2][3]=[6]_6=[0]$ and $[2][5]=[10]_6=[4] \Rightarrow [2][3]+[2][5]=[0]+[4]=[4]$ (as per Table- 13)

Thus L.H.S. = R.H.S. So distributive property also holds.

Thus $(I \text{ / mod } G, +)$ is an commutative ring. Moreover [1] will be identity element under modulo multiplication as well because $[1]\cdot[a]=[a]=[1][a]$ for any $a\in I \text{ / mod } 6$.

So one can say it is commutative ring with unity. But it is not integral domain. It is a ring with zero divisor since we have $[2]\neq[3]\neq 0$ but $[2][3]=[6]=[0]$ satisfying the condition of zero divisor given by $a\neq 0, b\neq 0 \Rightarrow ab=0$

Hence $(I \text{ / mod } 6\neq 0)$ is a commutative ring with unity with zero divisor.

NOTE

Remark : The student can see the behaviour of modulo system for integer m that when m is a prime number p and m is not a prime. In first case it is field as well as integral domain but in second case it is commutative ring with unity with zero divisor.

10.3 GENERAL CHARACTERISTIES OF RING

Similar to groups, we will discuss some general properties ring structure as given by the following theorem.

10.3.1. Theorem : The following conditions hold for any ring $(R, +, \cdot)$.

(a) $0a = 0 = a \cdot 0 \forall a \in R$

(b) $a(-b) = -(a \cdot b) = (-a) \cdot b \forall\ a, b \in R$

(c) $(-a)(-b) = a \cdot b \ \forall\ a, b \in R$

(d) $a(b - c) = ab - ac \ \forall\ a, b, c \in R$

Proof : (a) One can observe that this property similar to our number system when any number multiplied by 0 reduces it to zero. In the same way one see that when unity element of '+' as 0 is combined under any other non zero element of R under '$\cdot$' it reduces to identity to '+' as '0'. Now we will prove it by using the condition of ring structure and of group as follows. We will show that for $0a = 0 = a \cdot 0 \forall a \in R$. To prove it we will first consider $0a = 0$ of (a) and other part of (a) $a0 = 0$ can also be proved similarly. Now to prove the first part let us consider

	$a + 0 = a$	as 0 is identity for '+'	…(1)
	$0 + 0 = 0$	taking $a = 0$ in (1)	…(2)
$\Rightarrow$	$a(0 + 0) = a \cdot 0$	for any $a \in R$	…(3)
$\Rightarrow$	$ao + a0 = a \cdot 0$	Distributive property from left	…(4)
$\Rightarrow$	$a0 + a0 = a0 + 0$	Identity property for '+'	…(5)

Since $(R, +)$ is abelian group so it will satisfy cancellation law so by left cancellation law in (5), we have $a0 = 0$ hence $ao = 0$ holds. Similarly $0 \cdot a = 0$ can be shown by taking right cancellation law in $(0 + 0)a = 0 \cdot a + 0$ after simplification by following the steps (4) and (5).

The student note that $a0 = 0$ and $oa = 0$ has been proved separately because in general ring $(R, +, \cdot)$ may not be commutative under '+'.

(b) This property is again similar to the number system where if any number is multiplied by negative number, then the resulting number after multiplication becomes negative, just as $3(-2) = -6$ as $(-2)(3) = -6$. In a similar way the property stated in (b) indicates that for any $a \in R, -a \in R$ is additive inverse so when it combined with other element of R under '$\cdot$' will give the resulting element as the inverse of the combined elements under '+'. So to prove it again we will consider the first part of (b) given by. $a(-b) = -(ab)$. The other part $(-a)b = -(ab)$ can be proved similarly. Now to prove the first part let $b \in R$ be any arbitrary element then $-b \in R$ will be the inverse of $b \in R$ under '+' such that $b + (-b) = 0$. property of inverse …(6)

$\Rightarrow$	$a \cdot (b + (-b) = a \cdot 0$		
$\Rightarrow$	$a \cdot b + a(-b) = a \cdot 0$	Distributive property	…(7)
$\Rightarrow$	$a \cdot b + a(-b) = 0$	$\because\ a \cdot 0 = 0$ from (a)	…(8)
$\Rightarrow$	$a(-b) = -(a \cdot b)$	property of inverse	…(9)

Thus (b) condition holds.

(c) To prove $(-a)(-b) = ab$ we will make use of (b) property twice first so we have

$(-a)(-b) = -(-a)(b)$ by the property (9) …(10)

$\Rightarrow$ $(-a)(-b) = -(-(ab))$ by property $(-a)b = -(ab)$ …(11)

$\Rightarrow$ $= ab$ $\because$ $(a^{-1})^{-1} = a$ or $-(-a) = a$ …(12)

Hence by the inverse property group we have $(-a)(-b) = ab$ NOTE

Thus (c) condition hold.

(d) $a(b-c) = a(b+(-c))$ …(13)

$= ab + a(-c)$ Distributive property …(14)

$= ab - ac$ $\because$ $a(-c) = -ac$

Hence (d) condition holds.

10.4 CANCELLATION LAWS UNDER '·' BINARY OPERATION

Since we know that in ring structure $(R, +)$ is an abelian group so cancellation laws for '+' will holds, but $(R, \cdot)$ is a semi group so the condition of group can not be applied in $(R, \cdot)$. Then the question arises under what condition the cancellation law for $(R, \cdot)$ can hold. We will show that cancellation law under '·' from left (right) holds under the specific condition and in general it cannot be hold. Before we discuss the condition, let us first define the left (right) cancellations laws in ring $(R, +, \cdot)$ under '·' binary operation.

10.4.1 Definition : Let $(R, +, \cdot)$ be any arbitrary ring then for $a, b, c \in R$ the left (right) cancellation laws inder '·' is given by when $a \neq 0 \in R$ $ab = ac \Rightarrow b = c$ (left cancellation)

$ba = ca \Rightarrow b = c$ (right cancellation)

The following theorem gives the necessary and sufficient condition for cancellation laws in ring structure to hold.

10.4.2. Theorem : The left (right) cancellation laws in $(R, +, \cdot)$ hold if and only if R is a ring without zero divisor.

Proof : Condition is necessary (only if).

Suppose left (right) cancellation laws holds $(R, +)$

We claim $(R, +, \cdot)$ is a ring without zero divisor.

To prove we must show that for $a, b \in R$ $ab = 0$ $\Rightarrow$ either $a = 0$ and $b = 0$

To prove it suppose $a \neq 0$ then we will show that $b = 0$

To have this condition since we have $ab = 0$ (given)

$\Rightarrow$ $ab = a \cdot 0$ $\because$ $0 = a \cdot 0$

$\Rightarrow$ $b = 0$ (left cancellation law being hold)

Similarly we can be $b \neq 0$ then $a = 0$ by using right cancellation law condition in $ab = 0b$

Thus condition is necessary holds.

Condition is sufficient. Suppose $(R, +, \cdot)$ is a ring without zero division.

We claim it satisfies both left and right cancellation laws. To prove we must show that if $a, b, c \in R$ and $a \neq 0$ $ab = bc \Rightarrow b = c$ (1) and $ba = ca \Rightarrow b = c$ (2)

To prove (1) let us first consider $ab = bc, a \neq 0$ Then we must show $b = c$ holds

To prove it since we have $ab = ac$

$\Rightarrow ab - ac = 0$ Taking $-ac$ as an inverse of ac

$\Rightarrow a(b-c) = 0$ Distributive property

$\Rightarrow b - c = 0$ since $(R, +, \cdot)$ is ring without zero divisor and $a \neq 0$

$\Rightarrow b = c$

So left cancellation to hold similarly one can show that right cancellation law will hold. Hence condition is sufficient hold. Thus the theorem.

NOTE

10.5 SUBRING OF A RING

Like subgroups of a group we will now discuss subring of a ring defined as follows.

10.5.1. Definition : Let $(R, +, \cdot)$ be any arbitrary ring then any non-empty subset $S \in R$ is a sub ring if S under the binary operation of '+' '·' satisfies all the properties of ring.

To prove by this definition for any subset S of R to be subring one will have to prove all the properties of rings structure. To save this process we will again consider the necessary and sufficient condition given by the following theorem for any subset of ring to be subring.

10.5.2. Theorem : Let $(R, +, \cdot)$ be any arbitrary ring and $S \subseteq R$ be any subset of R. Then S is a subring if and only if for any $a, b \in S$ the following conditions hold

(i) $a - b \in S$

(ii) $a \cdot b \in S$

Proof : Condition is necessary : Suppose $S \subseteq R$ be a subgroup of $(R, +, \cdot)$.

We claim (i) and (ii) condition are satisfied.

To prove it since S is subgroup so it will satisfy all the properties of ring under '+' '·' of R.

So we have

(a) $(S, +)$ is abelian group.

(b) $(S, +)$ is semi group.

(c) '·' satisfies distributive property over '+'.

Now by (a) $(S, +)$ is abelian group so for any $b \in S$ will have additive inverse, $-b \in S$. so $a \in S$, $-b \in S \Rightarrow \; a - b \in S$ as S is closed under '+'. So (i) condition holds.

Again $a \in S \; b \in S \;\Rightarrow\; a \cdot b \in S$. Since by (b) S is semi group so S will be closed under '·'. Thus (i) and (ii) will hold. Hence condition is necessary hold.

Condition is sufficient : Suppose $S \subseteq R$ be such that for any $a, b \in R$ (i) and (ii) conditions hold. We claim S is a subring of R.To prove it we must show that

(a) $(S, +)$ is an abelian group.

(b) $(S, \cdot)$ is a semi group.

(c) Distributive '.' over '+' holds.

To prove (a) we will first prove that S has element $0 \in S$.

To prove it since by (i) we have for any $a, b \in S \Rightarrow a - b \in S$. Taking $b = a$

$$\text{we have } a, a \in S \;\Rightarrow a - a \in S$$
$$\Rightarrow 0 \in S$$

So additive identity 0 exists in S of R.

Again taking $a = 0, b = 0$ (i) we have $\quad 0 - a \in S \Rightarrow -a \in S$

So each $a \in S$ has its additive inverse is S

Now $a \in S, b \in S \;\Rightarrow -b \in S$ so by condition (i) $\Rightarrow \; a - (-b) \in S$

$$\Rightarrow a + b \in S$$

So S is closed in S under '+'

Now S being sub set of R so every member of S being number of R and R satisfies associative and commutative properties under '+' so the member of S being member of R will also satisfy associative and commutative properties under '+' thus $(S, +)$ will become abelian group.

Hence (a) condition hold.

To prove (b) Again since by (ii) S is closed under '$\cdot$' and $S \subseteq R$ so every member S being member of R will satisfy associative property under '$\cdot$' of R. So $(S, \cdot)$ will be a semi group.

NOTE

So (b) condition holds. Similarly S being closed under '+' and '$\cdot$'. So S will satisfy the distributive properties of '$\cdot$' over '+'.

So (c) condition will also hold. Thus $(S, +, \cdot)$ satisfies all (a), (b), (c) condition for ring so $(S, +, \cdot)$ must be a subring of R.

10.5.3. Sub-field of a Field : Similar to sub group and subring, we can also consider subfield of field as any non-empty subset K of a field F will be subfield if K satisfies all the conditions of field under '+' and '$\cdot$' of F. The necessary and sufficient condition for any subset of K of F to be field can be similarly stated as follows.

10.5.4. Theorem : Any non-empty subset K of a field F is a subfield if any only if for any $a, b \in K$ the following condition hold (i) $a - b \in K$ (ii) $a \cdot b^{-1} \in K$.

The proof is similar to subring so left as exercise to the students.

10.5.5. Characteristics of subring : We will state some of the properties of subring which are a quite similar to the properties of subgroups given by the following theorem.

10.5.6. Theorem : The following properties hold for any subring of ring $(R, +, \cdot)$

(a) The union of two subrings may not necessarily be a subring.

(b) The intersection of two subgroups as always a subring.

(c) The arbitrary intersection of subgroups is always a subring.

(d) The union of two subrings in a subring if and only of either of the subring is the subset of other.

Proof : (a) This condition can be again, shown by taking the same examples as we have taken for the subgroup in (a) of theorem 9.3.11 by having I_3, I_4 as subgroups of $(I, +)$ given by

$$I_3 = [0, \pm 3, \pm 6, \pm 9, \ldots] \quad \ldots(1) \qquad I_4 = [0, \pm 4, \pm 8, \pm 12, \pm \ldots] \quad \ldots(2)$$

As we have shown that I- set of integer is also commutative ring under '+' and '$\cdot$' binary operation and we know I_3, I_4 are subgroup under '+'. Now we show that they are also subring by showing that they are closed under multiplication by taking x, y being two member of either of I_3 or I_4 let $x = ma$, $y = nb$ for some $a, b \in I$ where m can be 3 or 4 because I_3, I_4 are multiple of 3, 4 of the members of I and m is also member of I.

Now $xy = mamb = m(mab)$ as $m, a \in I$. I is commutative under multiplication so $am = ma$.

Now $ma \in I, b \in I \Rightarrow mab \in I$. So we have $xy = mamb = m(mab)$

$\Rightarrow m(mab) \in$ Im for any $m = 3$, or $4 \Rightarrow xy \in I_m$ where m can be either 3 or 4. Hence I_3 *or* I_4 is closed under multiplication.

Thus I_3 and I_4 are closed under multiplication. So I_3, I_4 are subring of $(I, +, \cdot)$

But $I_3 \cup I_4 = [0, \pm 3, \pm 4, \pm 6, \pm 8, \ldots]$ is not closed under '+' as $3, 4 \in I_3 \cup I_4$ but $3 + 4 = 7 \notin I_3 \cup I_4$. Hence $I_3 \cup I_4$ is not qualified for subring. Thus (a) condition holds.

(b) Let S, T be any two subring. Then we claim $S \cap T$ is a subring.

To prove it let $a, b \in S \cap T$ be any two member then $a, b \in S$ and $a, b \in T$

Since S and T are each subring so by the sufficient condition of subring we have

$$a, b \in S \Rightarrow a - b \in S \text{ and } ab \in S \quad \ldots(1)$$

Similarly when $a, b \in T \Rightarrow a - b \in T$ and $ab \in T$ $\ldots(2)$

So from (1) and (2) we have $a - b \in S$ and T and $ab \in S$ and T

NOTE

Thus for any $a, b \in S \cap T \Rightarrow a - b \in S \cap T$ and $ab \in S \cap T$

hence $S \cap T$ must be sub ring. Thus thus the intersection of any two sub rings is always a subring. Hence (b) condition holds.

(c) This can be proved similarly as that of (b) by taking $[S_l : l \in \wedge]$ as arbitrary collection of subrings of any $(R, +, \cdot)$

We claim $\underset{X \in \wedge}{\cap} S_l$ is a sub ring.

To prove it let $a, b \in \underset{l \in \wedge}{\cap} S_l \Rightarrow a, b \in S_l$ for each $x \in \wedge$

$\Rightarrow a - b \in S_l$ and $ab \in S_l$ as each S_l is a sub ring for each $l \in \wedge$.

$\Rightarrow a - b, ab \in \underset{l \in \wedge}{\cap} S_l$ by definition of Intensection of set.

$\Rightarrow \underset{l \in \wedge}{\cap} S_l$ must be a sub ring.

Thus the arbitrary intersection of sub rings sub ring.

10.5.7. Examples on Subgroups : The examples of subring again, like subgroup, normal subgroups classified into two types.

(a) Improper subring

(b) Proper subring

(a) Improper subring : Here, like sub grops, normal subgroups. The ring R itself as a subset and the subset consists of only identy element [0] under '+' are the only improper subrings of any ring $(R, +, \cdot)$ as they are only set improper subgroup of R.

(b) Proper subring : All subrings other than [0] and R are classified as proper subring. The examples of proper subring can again of two types.

(I) Infinite subring (II) Finite subring.

(I) Infinite subring : As we know that the infinite set of numbers satisfy $I \subset Q \subset R \subset C$ so

(1) $(I, +, \cdot)$ is a subring of rings Q, R and C.

(2) $(Q, +, \cdot)$ is a subring of rings R and C

(3) $(R, +, \cdot)$ is a subring of C.

(4) $I\,m$ is a subring of $(I, +, \cdot)$. where $I_m = \{ma : a \in R\}$ where m is any positive integer.

(5) Let $M_2(R)] = \{A : A = (a_{ij})_{2\times 2}\}$ be set of 2×2 matrices set of real number R.

Then $S = \left\{ \begin{bmatrix} x, & 0 \\ 0, & 0 \end{bmatrix} = x \in R \right\}$ is a subring of $M_2(R)$, as seen by taking any two member

$A = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} y & 0 \\ 0 & 0 \end{bmatrix}$ be any two matrices of S for any $x, y \in R$.

We should test for (i) $A - B \in S$ (ii) $AB \in S$

Now $A - B = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} y, & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} x - y & 0 - 0 \\ 0 - 0 & 0 - 0 \end{bmatrix} = \begin{bmatrix} x - y & 0 \\ 0 & 0 \end{bmatrix}$ as $x, y \in R \Rightarrow x - y \in R$

Let $x - y = z \in R$ then $A - B = \begin{bmatrix} z & 0 \\ 0 & 0 \end{bmatrix} \in S$ by definition of S. So (i) condition holds.

Again let us consider $AB = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} y & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} xy + 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} xy & 0 \\ 0 & 0 \end{bmatrix}$ $x, y \in R \Rightarrow xy \in R$

Let $xy = k \in R$ so we have $AB = \begin{bmatrix} k & 0 \\ 0 & 0 \end{bmatrix} \in S$ So (ii) condition holds.

Thus S is a subring of $M_2(R)$

NOTE

(II) Examples on Finite Subring : Since we have shown that only modulo sets are qualified to become finite ring as well as finite field when p is a prime number when $m = p$ under $a \equiv b$ mod m. (See example (i) and (ii) in 10.2.2 for Finite Ring/Field). Again, we have shown from example 4 and 5 on modulo group under 8.3.4. and its extension 8.3.5 that when $m = p$ is some prime number then it has no subgroup under modulo addition (see example (i) as proper finite subgroup (II) under 9.2). But it has one proper subgroup under modulo multiplication. Hence it will not be a subring under $a \equiv b$ mod m when m is some prime number and also it will not be proper subfield. However if $a \equiv b$ mod m is not prime number but some composite number like 4, 6, 8 etc then it has proper subgroup under addition but is has no subgroup under modulo multiplication because non-zero residue classes of composite number do not form a group under medulo multiplication, so they cannot be consider field, but we have shown that such set of these residue classes including [0] class becomes commutative ring with unity as can be seen from the example (ii) on modulo system in 10.2.2. So if we consider the same example of ring under modulo 6, and take two sub groups

$H = \{[0], [2], [4]\}$ …(1) and $K = \{[0], [3]\}$ …(2)

Proved under modulo addition. Now let us check they are semigroups under modulo multiplication or not by constructing composition tables for (1) and (2) respectively as shown below.

Composition table for H under modulo 6.

·	[0]	[2]	[4]
[0]	[0]	[0]	[0]
[2]	[0]	[4]	[2]
[4]	[0]	[2]	[4]

(Table - 14 for H)

·	[0]	[3]
[0]	[0]	[0]
[3]	[0]	[3]

(Table - 15 for K)

In both there tables for H and K under modulo multiplication for modulo 6, each one closed and each will satisfy associative property under multiplication. So both H, K are sub ring of finite ring under modulo 6. Moreover, they are commutative as well but has no identity element [1]. So they are commutative subring. Thus whenever there is modulo rings under composite number then there will be subrings of it.

10.6 IDEALS OF RING

Now we will derive very important concept called as Ideals under rings structure which plays very important role like normal sub group under group defined as follows.

10.6.1. Definition : Let $(R, +, \cdot)$ be any arbitrary ring let $S \subseteq R$ be any arbitrary non empty subset of R then S is said to be an ideal of R if S satisfies the following.

NOTE

(a) S is a subgroup of R

(b) for $a \in S$ and $r \in R \Rightarrow ar \in S$ and $ra \in S$

In condition if $ar \in S$ but $ra \notin S$ then S is said to be right ideal of R and in case $ar \notin S$ but $ra \in S$ then S is said to be left ideal of R. Thus like left (right) cosets of H, we have left (right) ideals of R.

10.6.2. Examples on Ideals : Like subgroup and subring again [0] and R are considered as Improper ideals of R and all other ideals as proper ideals of R. We will consider some examples of proper ideals of R as well as of left (Right) ideals of R.

16.6.3. Examples of Infinite proper ideals : We have shown in examples of subring under. Infinite proper sub ring that $(I, +, \cdot)$ is subring of $(Q, +, \cdot)$, $(C, +, \cdot)$, $(Q, +, \cdot)$ is subring of $(R, +, \cdot)$ and $(C, +, \cdot)(Q, +, \cdot)$ is sub ring of $(R, +, \cdot)$ and $(C, +, \cdot)$.

Any subset to be ideal first condition is that to should be subring. So (a) condition holds but none of them for ideal qualifies because through $(I, +, \cdot)$ is a subgroup of $(Q, +, \cdot)$, $(R, +, \cdot)$, $(C, +, \cdot)$ but $n \in I$ and element from Q, R, C.

When combined with n as under $nr \notin I$. Similar $(Q, +, \cdot)$ will not be ideal of $(R, +, \cdot)$ and $(C, +, \cdot)$ and $(R, +, \cdot)$ will ideal of $(C, +, \cdot)$. However we have shown that set even number $I_2 = [0, \pm 2, \pm 4, \ldots]$ is a sub ring of $(I, +, \cdot)$. Now it is also ideal of $(I, +, \cdot)$, because of take n from I and multiply with any number from set of even number I_2, it will be again even number, because any even is multiple of 2 and any number multiplied by 2 will always be even so it will be closed from left as well as from right, that is $n \in I$ and for $a \in I_2 \Rightarrow na, an \in I_2$

Thus I_2 is a proper ideal of $(I, +, \cdot)$. Not only I_2 but we will show that it holds for any I_m for any given positive integer n by the following example

Example 1. : Let $I_m = \{ma : a \in I\}$ as stated is 10.5.7. It can be shown that I_m is an ideal of I by proving that

(a) I_m is a subring.

(b) For $x \in I_m$ and $n \in I$, $nx \in I_m$, $xn \in I_m$

To prove (a) we will show that if $x, y \in I_m$ be any arbitrary member of I_m then

(i) $x - y \in I_m$

(ii) $xy \in I_m$

Now to prove (i) since $x, y \in I_m$ so $x = ma$, $y = mb$ for some $a, b \in I$ then

$x - y = ma - mb = m(a - b)$ Now $a, b \in I \Rightarrow a - b \in I$, since I is closed under difference.

$\Rightarrow m(a - b) \in I_m$ by definition of I_m

$\Rightarrow x - y \in I_m$

So (i) condition holds

Again to prove (ii) $xy = ma \cdot mb$

$= m(am) \cdot b$ I is Associative

$= m(ma)b$ I is commutative

$= m(m(ab))$ I is Associative

$= m(mab)$ Now $a, b \in I$ $ab \in I$ & $m \in I \Rightarrow mab \in I$

$= mk$ Let $mab = k, \Rightarrow k \in I$

$\Rightarrow mk \in I_m$ $m \in I, k \in I \Rightarrow mk \in I_m$

$\Rightarrow xy \in I_m$

So (ii) condition hold. Hence I_m is a subring of $(I, +, \cdot)$

So (a) condition hold. To prove (b). Let $x = ma$, let $x \in I$ be any arbitrary element, then

$$nx = n(ma) = (nm)a = (mn)a \quad \text{commutative condition}$$

$$= m(na)$$

$$a \in I \; n \in I \Rightarrow na \in I \Rightarrow m(na) \in I_m$$

$$\Rightarrow nx \in I_m$$

Similarly $xn = man = m(an) = m(na)$ Now $an = na \in I$, Since I is commutative under '$\cdot$'

$$\Rightarrow m(na) \in I_m$$

$$\Rightarrow xn \in I_m$$

Hence (b) condition holds thus I_m satisfies (a) and (b) conditions so I_m is at proper. Infinite ideal of I.

10.6.4. Examples of Infinite left (right) ideal we will consider some examples of left (right) ideal ring as given below.

Example 1. Let $M_2(I)$ be ring of all matrices of type 2×2 having element of integer from I and left $S = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} = a, b \in I \right\}$ be subset of $M_2(I)$ of 2×2 matrices. Then S is left ideal but not right ideal of $M_2(I)$.

Solution. To prove S is a left ideal of $M_2(I)$ we must show that of $A, B \in S$ being two matrices of S then

(a) S sub ring $M_2(I)$

(b) any $T \in M_2(I)$ and $A \in S$

$$TA \in S \text{ but } AT \notin S$$

To prove (a) We must show that for $A, B \in S$

(i) $A - B \in S$

(ii) $AB \in S$

To prove (i) since $A, B \in S$ let $A = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}, B = \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix} a_1, b_1, a_2, b_2 \in I$

Then $A - B = \begin{bmatrix} a_1 - a_2 & 0-0 \\ b_1 - b_2 & 0-0 \end{bmatrix} = \begin{bmatrix} a_1 - a_2 & 0 \\ b_1 - b_2 & 0 \end{bmatrix}$

$a_1, a_2 \in I \Rightarrow a_1 - a_2 \in I$ and $b_1, b_2 \in I \Rightarrow b_1 - b_2 \in I$ so difference any two integers always an integer. Therefore $\begin{bmatrix} a_1 - a_2, & 0 \\ b_1 - b_2, & 0 \end{bmatrix} \in S \Rightarrow A - B \in S$

So (i) condition hold. To prove (ii) we have $AB = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} \begin{bmatrix} b_1 & 0 \\ b_2 & 0 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & 0 \\ b_1 a_2 & 0 \end{bmatrix}$

$a_1, a_2 \in I \Rightarrow a_1 a_2 \in I$ and $b_1 \in I \, b_2 \in I \Rightarrow b_1 b_2 \in I$ Since I is closed under multiplication and therefore $\begin{bmatrix} a_1 a_2 & 0 \\ b_1 b_2 & 0 \end{bmatrix} \in S \Rightarrow AB \in S$

So (ii) condition hold.

Hence S satisfies (i) and (ii) condition for subsring so S must be subring of $M_2(I)$.

NOTE

NOTE

To prove S is left ideal let $T \in M_2(I)$ be any arbitrary 2×2 matrix given by $T = \begin{bmatrix} p & q \\ r & s \end{bmatrix} p, q, r, s \in I$

Let $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \in S$ being member of S. Therefore $TA = \begin{bmatrix} ap+bq & 0 \\ ra+bs & 0 \end{bmatrix} a, b \in I$

Now $ap + bq \in I$ $ra + bs \in I$ so $TA = \begin{bmatrix} ap+bq & 0 \\ ra+bs & 0 \end{bmatrix} \in S$

So (b) condition holds for S. Hence S is left ideal of $M_2(I)$.

but S is not right ideal of $M_2(I)$ because of we consider

$$AT = \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ap+r & aq+0 \\ bb+0 & bq+0 \end{bmatrix}$$

$$= \begin{bmatrix} ap & aq \\ bb & pq \end{bmatrix} \notin S$$

Hence, S is not right ideal of $M_2(I)$.

Example 2. In example 1 if $S = \left\{ \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}, a, b \in I \right\}$ then student can easily verify that S is right ideal of $M_2(I)$ but not left ideal of $M_2(I)$. *[M.L. univ. Jan 2008]*

10.7 CHARACTERISTICS OF IDEALS OF RING

Theorem : The following condition hold for the ideals of any ring $(R, +)$.

(a) The union of two ideals may not necessarily be idea.

(b) The intersection of two ideals is always an ideal.

(c) The arbitrary intersections of ideals of an ideal.

(d) The union of two ideals is either of them is the subset of other.

(e) If A, B be any two ideals if R. Let $A + B = [z = z = a + b \; a \in A, b \in B]$

Then $A + B$ is an ideal of R such that A, B are both subset of $A + B$. That is sum of any two ideals is an ideal such that either of the ideal is the subset of sum of the ideals.

Proof : Since most of properties also similar to subgroups and subring so they can be proved in similar manner except (e), we will prove (e) under solved examples.

10.8 CONCEPT OF HOMO IN RING STRUCTURE

We conclude this chapter by defining the concept homomorphism is ring structure which also held for field as well defined as given below.

10.8.1. Definition : Let $(R, +, \cdot)$ and $(R^*, +, \cdot)$ be any two arbitrary ring. Then any mapping $f : R \to R^*$ defined between $(R, +, \cdot)$ to $(R^*, +, \cdot)$ is homomorphism if for any $a, b \in R$, f satisfies the following.

(a) $f(a + b) = f(a) + f(b)$

(b) $f(ab) = f(a) f(b)$

The other concepts such as monomorphism, epimorphism and isomorphism can be defined as they have been defined for group structure by just replacing group G, G^* by ring R, R^* in each of the definition stated there.

10.8.2. Basic properties of homomorphism : These properties are again similar to group theory and can be proved similarly given by the following theorem.

10.8.3. Theorem : Let $f : R \to R^*$ be any monomorphism defined from $(R, +, \cdot)$ to $(R^*, +, \cdot)$ then following properties hold for f.

(a) $f(0) = 0^*$

(b) $f(-a) = -f(a)$ any $a \in R$

where '0' and '0^*' are be additive identity of R and R^* respectively and $-a \in R$ is additive inverse of $a \in R$.

NOTE

Solved Examples

Example 1. If $a, b \in R$ where R is a ring then prove that

$$(a+b)^2 = a^2 + ab + ba + b^2$$

Solution. Since we know that ring is not commutative under '$\cdot$' so $ab \neq ba$ for $a, b \in R$

$$\begin{aligned}
(a+b)^2 &= (a+b)(a+b) && \text{By definition of integral power.}\\
&= (a+b)a + (a+b)b && \text{Distributive property from left}\\
&= a \cdot a + ba + a \cdot b + b \cdot b && \text{Distributive property from right}\\
&= a^2 + ba + ab + b^2
\end{aligned}$$

Example 2. If $(R, +, \cdot)$ be a ring with unity such that

$$(xy)^2 = x^2 y^2 \ \forall\ x, y \in R$$

Then prove that R is commutative.

Solution. Since R is ring with unity so $1 \in R \Rightarrow y + 1 \in R$ for any $y \in R$, so we have

$$\begin{aligned}
(x(y+1))^2 &= x^2 (y+1)^2 && \text{By given hypothesis } (xy)^2 = x^2 y^2 && \ldots(1)\\
&= x^2 (y+1)(y+1) && \text{By definition of Integral power} && \ldots(2)\\
&= x^2 ((y+1)y + (y+1)1)) && \text{Distributive property from left} && \ldots(3)\\
&= x^2 (yy + y + y + 1) && \text{Distributive property from right} && \ldots(4)\\
&= x^2 (y^2 + y + y + 1) && && \ldots(5)\\
&= x^2 (y^2 + 2y + 1) && &&\\
&= x^2 y^2 + 2x^2 y + x^2 && \text{Distributive property} && \ldots(6)
\end{aligned}$$

But $(x(y+1))^2$ can also be expressed as

$$\begin{aligned}
x(y+1)x(y+1) && \text{By definition of Integral power} && \ldots(7)\\
= (xy + x)(xy + x) && \text{Distributive from left} && \ldots(8)\\
(xy + x)xy + (xy + x)x && \text{Distributive from right} && \ldots(9)\\
xyxy + xxy + xyx + xx && \text{Distributive from right} && \ldots(10)\\
= (xy)^2 + x^2 y + xyx + x^2 && && \ldots(11)
\end{aligned}$$

Thus from (7) and (11) we have

$$(xy)^2 + x^2 y + xyx + x^2 = x^2 y^2 + x^2 y + x^2 y + x^2 \quad \ldots(12)$$

Since $(R, +, \cdot)$ is and abelian group so it satisfies cancellation laws, both from left and right under '+' since $(xy)^2 = x^2 y^2$ given, so we have

$$x^2 y^2 + x^2 y + xy + x^2 = x^2 y^2 + x^2 y + x^2 y + x^2 \quad \ldots(13)$$

$$xyx = x^2 y \quad \text{(By left and right cancellation laws)} \quad \ldots(14)$$

Now again, replacing x by $x + 1$ in (14), we have

NOTE

$$(x+1)y(x+1) = (x+1)^2 y \quad \ldots(15)$$

$$(xy+y)(x+1) = (x+1)(x+1)y \quad \text{Distributive from right} \quad \ldots(16)$$

$$(xy+y)x + (xy+y)1 = ((x+1)x + (x+1)y) \quad \text{Distributive from left \& right} \ldots(17)$$

$$xyx + yx + xy + y = (x+1)x + (x+1)y \quad \text{Distributive from right} \quad \ldots(18)$$

$$x^2 y + yx + xy + y = (x^2 + x + xy + y) \quad \text{Taking } xyx = x^2 y \text{ from (14)} \quad \ldots(19)$$

$$x^2 y + yx + xy + y = x^2 y + xy + xy + y \quad \text{By applying cancellation law} \quad \ldots(20)$$

$$yx = xy$$

Proving that R is commutative.

Example 3. $(R, +, \cdot)$ be a ring such that $a^2 = a \; \forall \; a \in R$ prove that

(i) $a + a = 0 \; \forall \; a \in R$ is each element of R

(ii) $a + b = a \Rightarrow a = b$

(iii) R is a commutative ring.

Solution. Here $(R, +, \cdot)$ is a ring satisfying Idempotent condition $a^2 = a \; \forall \; a \in R$, *i.e.*, R is Boolean ring then we have to prove that it satisfies (i), (ii) and (iii) of given problem.

To prove (i) since $a \in R \Rightarrow a + a \in R$ Since R is closed under '+'

But

$$(a+a)^2 = a + a \quad \text{by given condition} \quad \ldots(1)$$

$$(a+a)(a+a) = a + a \quad \text{Integral power property} \quad \ldots(2)$$

$$(a+a)a + (a+a)a = a + a \quad \text{Distributive property from left} \quad \ldots(3)$$

$$(aa + aa) + aa + aa = a + a \quad \text{Distributive property from right} \ldots(4)$$

$$(a^2 + a^2) + (a^2 + a^2) = a + a \quad \because aa = a^2 \quad \ldots(5)$$

$$(a+a) + (a+a) = (a+a) \quad a^2 = a \text{ (by given hypothesis)} \quad \ldots(6)$$

$$(a+c) + (a+a) = (a+a) + 0 \quad \text{Identity property} \quad \ldots(7)$$

$$\Rightarrow \quad (a+a) = 0 \quad \text{left cancellation law in '+'} \quad \ldots(8)$$

$\Rightarrow$ a must be its own inverse. So (i) condition holds.

To prove (ii) we have let $a + b = 0$ given

We have to prove $a = b$

To prove it since $a + b = 0 \Rightarrow a + b = a + a$ from (8) …(9)

$$\Rightarrow \quad b = a \quad \text{By left cancellation law} \quad \ldots(10)$$

$$\Rightarrow \quad a = b \quad \text{Equality is symmetric} \quad \ldots(11)$$

So (ii) condition holds.

To prove (iii) that R is commutative we must show that $\forall \; a, b \in R \Rightarrow \; ab = ba$

To prove it since $a, b \in R \Rightarrow a + b \in R$

$$\Rightarrow \quad (a+b)^2 = a + b \quad \text{By given hypothesis}$$

$$(a+b)(a+b) = a + b \quad \text{Integral power property} \quad \ldots(12)$$

$$(a+b)a + (a+b)b = a + b \quad \text{Distributive property from left} \quad \ldots(13)$$

$$aa + ba + ab + bb = a + b \quad \text{Distributive property from right} \quad \ldots(14)$$

$$a^2 + ba + ab + b^2 = a + b \quad \because aa = a^2 \quad \ldots(15)$$

$$a + ba + ab + b = a + b \quad a^2 = a \text{ (by given hypothesis)} \quad \ldots(16)$$

$$ba + ab = 0 \quad \text{By left and right cancellation} \quad \ldots(17)$$

$$\Rightarrow \quad ab = ba \quad \text{By property (11) } a + b = 0 \Rightarrow a = b \quad \ldots(18)$$

So R must be commutative.

Example 4. Every field is an integral domain but its converse is not always true.

Solution. Let $(F, +, \cdot)$ be any arbitrary field

We claim (i) $(F, +, \cdot)$ is integral domain.

NOTE

(ii) Converse of(i) does not always hold.

To prove (i) We must show that F is a commutative ring with unity without zero divisor. So to have then condition since F is a field so F is also abelian group under '$\cdot$' under its non-zero element. As F is commutative ring with unity. Therefore to prove F is integral domain, it is sufficient to show that F is ring without zero divisor. To have this condition let $a, b \in F$ being arbitrary elements such that $ab = 0$

We claim either $a = 0$ or $b = 0$

To prove it suppose $a \neq 0$ then we will show $b = 0$. To have this condition since F is an abelian group under '$\cdot$' of non-zero element each $a \in F$ has its inverse $a^{-1} \in F$ such that $aa^{-1} = 1 = a^{-1}a$. Since $a \neq 0 \Rightarrow a^{-1} \in F$, so we have

$$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}a$$

$$(a^{-1}a)b = a^{-1}0 \qquad \text{By associative property}$$

$$1 \cdot b = a^{-1}0 \qquad \text{By G- 4 condition}$$

$$b = 0 \qquad \because \quad a0 = 0 \; \forall \; a \in R$$

Thus if $ab = 0$ and $a \neq 0$, than we have shown $b = 0$

Similarly we can show that is $b \neq 0$ then $a = 0$

Thus proving that $(F, +, \cdot)$ is an integral domain. So (i) condition hold.

To prove (ii) we have already explained that $(I, +)$ is an integral domain but is not a field under the examples highlighting different types of Rings under 10.1.5.

Example 5. Since every integral domain may not field but there is particular condition under which integral domain becomes a field given by following theorem.

Theorem : Every finite integral domain is a field.

Solution : Let $(D, +, \cdot)$ be any finite integral domain let $D = \{a_1, a_2, \ldots, a_n\}$ has n elements. We claim $(D, +, \cdot)$ is a field.

Since $(D, +, \cdot)$ is an integral domain the D must be commutative ring without zero divisor. To prove $(D, +, \cdot)$ is a field we must show

(i) D has a Identity element called unity element under '$\cdot$'.

(ii) Every $0 \neq a \in D$ has its inverse in D..

To prove it as D is an integral domain so it is closed under '$\cdot$' therefore if $a \in D$ be any non-zero element then $aa_i \in D$ for $i = 1, 2, \ldots, n$. Thus we have

$D = \{aa_1, aa_2, \ldots, aa_i, aa_j, aa_n\}$ as the set of all the same n elements in some other order. We claim all these elements are again distinct.

To prove it suppose the claim is not true then $\exists \; aa_i, aa_j \in D$ such that

$$aa_i = aa_j \; i \neq j$$

$$\Rightarrow \quad aa_i - aa_j = 0$$

$$\Rightarrow \quad a(a_i - a_j) = 0 \qquad \text{since } a \neq 0 \text{ and } D \text{ is ring without zero divisor.}$$

$$\Rightarrow \quad a_i - a_j = 0$$

$$\Rightarrow \quad a_i = a_j$$

NOTE

Contradicting the condition that $a_i \neq a_j$

This contraction is due to over supposition that the claim is false hence this contradition proves that all the elements are distinct, so they will be same n element expressed in some other order. Therefore as $a \in D$ therefore a must be one among the new set of element let aak is such that $aak = a$ for some k …(1)

We claim ak is the unity (unit element as 1). To prove it let $a_j \in D$ be any arbitrary element. We claim $a_k a_j = a_j$

To have this condition since $a_j \in D$ so it must be one of the element under new set of elements let

$a_j = aa_i$ for some i. … (2)

Now let us consider

$a_k a_j = a_k(aa_i)$ from (2) …(3)

$= (a_k a)a_i$ D being Associative …(4)

$= (aa_k)a_i$ D is commutative …(5)

$= aa_i$ by (1) …(6)

$= a_j$ by (2) …(7)

Thus the a_k is the unit element is D which is unique let us denote $a_k = 1$. So $1 \in D$. Hence (i) condition holds.

To prove (ii) since $1 \in D$ so there must be some $aa_i \in D$ such that

$aa_i = 1 = a_i a$ D is commutative

$\Rightarrow a$ has inverse a for with respect '$\cdot$' D since $a \in D$ is any arbitrary non-zero element so each element of D has its inverse in D. So (ii) condition holds. Thus D satisfies (i) and (ii) so D must be field proving that every finite integral domain is always a field.

Example 6. Show that $S = [x : x = a + b\sqrt{2}, a, b \in I]$ is an integral domain but not a field under order '+' and '$\cdot$' multiplication.

Solution. To prove S is an integral domain we must show that

(a) $(S, +)$ is abelian group.

(b) $(S, .)$ is commutative semi group with unity.

(c) $(S, \cdot)$ satisfies the condition that S is a ring without zero divisor.

To prove (a) and (b) first we must show that it is closed under '+' and '$\cdot$'.

To have these condition let $x = a + b\sqrt{2}, y = c + d\sqrt{2}, a, b, c, d \in I$

Then $x + y = (a + b\sqrt{2}) + (c + d\sqrt{2})$

$= (a + c) + (b + d)\sqrt{2}$ by commutative and associative properties hold under I.

Now $a, c, b, d \in I \Rightarrow a + c \in I\ b + d \in I$ I is closed under '+'

$\Rightarrow (a + c) + (b + d)\sqrt{2} \in S$ By definition of S So $x + y \in S$

Hence S is closed under '+'.

Again let us consider $xy = (a + b\sqrt{2})(c + d\sqrt{2})$

$= (a + b\sqrt{2})c + (a + b\sqrt{2})(d\sqrt{2})$ Distributive property from left

$= ac + (b\sqrt{2})c + ad\sqrt{2} + (b\sqrt{2})d\sqrt{2})$ Distributive property from right

$= ac + bc\sqrt{2} + ad\sqrt{2} + bd(\sqrt{2})(\sqrt{2})$ By G -2 and G-5 condition

$= ac + bc\sqrt{2} + ad\sqrt{2} + 2bd$

$= (ac + 2bd) + (bc + ac)\sqrt{2}$ By G -2 and G-5 condition

Now $a, b, c, d \in I$ and I is closed under multiplicable and addition. So we have

$ac + 2bd \in I,\ bc + ad \in I \Rightarrow ac + 2bd + (bc + dd)\sqrt{2} \in S$ By definition of S

$\Rightarrow \quad xy \in S$

Thus S is closed under '$\cdot$' as well as since S is closed both under '+' and '$\cdot$'. So we can proceed to prove other condition under '+' and '$\cdot$' of S under (a) and (b) where we have to show S is abelian group under '+' and abelian semigroup under '$\cdot$'. Now we will first consider all properties of group under '+'.

$(G-2)$ To prove S is associative let $x, y, z \in S$ be such that $x = a + b\sqrt{2},\ y = c + d\sqrt{2}$

$z = e + f\sqrt{2}$ for $a, b, c, d, e, f \in I$

We claim $(x + y) + z = x + (y + z)$

To prove let us consider LHS of claim then we have

$(x + y) = (a + b\sqrt{2}) + (c + d\sqrt{2})$ ...(1)

$= (a + c) + (b + d)\sqrt{2}$ By G -2 and G-5 condition ...(2)

$\Rightarrow \quad (x + y) + z = ((a + c) + (b + d)\sqrt{2}) + (e + f\sqrt{2})$ ...(3)

$\Rightarrow \quad = (a + c) + e + ((b + d) + f)\sqrt{2}$ By G -2 and G-5 condition ...(4)

Since I is associative under '$\cdot$' so we have

$(a + c) + e = a + (c + e)$ ...(5) $(b + d) + f = b + (d + f)$ ...(6)

So from (5), (6), (4) becomes

$$\begin{aligned}(x + y) + z &= a + (c + e) + (b + (d + f))\sqrt{2} \\ &= a + (c + e) + (b + (d + f)\sqrt{2}) \\ &= (a + b\sqrt{2}) + ((c + e) + (d + e)\sqrt{2}) \\ &= (a + b\sqrt{2}) + ((b + d\sqrt{2}) + (c + e\sqrt{2})) \\ &= x + (y + z) \\ &= \text{R.H.S. of the claim.}\end{aligned}$$

Hence S is associative

***G* – 3 Existence of Additive Identity :** Since $0 \in I$ so $0 + 0\sqrt{2} \in S$

We claim $(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = a + b\sqrt{2} = (0 + a\sqrt{2}) + (a + b\sqrt{2})$

To prove it lt us consider $(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = (a + 0) + (b + 0)\sqrt{2}$

$= a + b\sqrt{2} \quad \because a + 0 = a$ and $b + 0 = b$

$= (0 + a) + (0 + b)\sqrt{2}$

have $0 + 0\sqrt{2}$ is an identity element in S under '+'.

(*G* – 4) Existence of Additive inverse : Since $a, b \in I$ so $-a, -b \in I$ such that

$a + (-a) = 0,\ b + (-b) = 0$ So $-a, + (-b)\sqrt{2} \in S$ By definition of S

We claim $(a + b\sqrt{2}) + (-a + (-b)\sqrt{2}) = 0 + 0\sqrt{2} = (-a + (-b)\sqrt{2}) + (a + b\sqrt{2})$

To prove it we have

$(a + b\sqrt{2}) + (-a + (-b)\sqrt{2}) = (a + (-a)) + (b + (-b)\sqrt{2}$

$= 0 + 0\sqrt{2} \quad \because a + (-a) = 0 \,\&\, b + (-b)$

$= (-a - b)(\sqrt{2}) + (0 + b\sqrt{2})$

hence $-a + (-b)\sqrt{2}$ i additive inverse of $a + b\sqrt{2}$.

NOTE

$G-5$ Commutative properly : Let $x = a + b\sqrt{2}$ $y = b + d\sqrt{2}$ be any pair of elements then we claim $x + y = y + x$

NOTE

To prove it let us consider $x + y = (a + c) + (b + d)\sqrt{2}$

But I is commutative under '+'. So we have $a + c = c + a$ $b + d = d + b$ therefore,

$$x + y = (a + c) + (b + d)\sqrt{2} = (c + a) + (d + b)\sqrt{2}$$
$$= (c + d\sqrt{2}) + (a + b\sqrt{2})$$
$$= (y + x)$$

Thus $(S, +)$ is commutative abelian group. Hence (i) condition hold.

To prove (ii) since S is proved to be closed under '$\cdot$'. So it remains to show that S is associative under '$\cdot$'. To have this condition we will show that $(xy)z = x(yz)$

where $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$ $z = e + f(\sqrt{2})$ to prove the condition let us first consider

$xy = (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2}$ already proved under closed condition.

Let $ac + 2bd = m$ and let $bc + ad = n$ then we have $xy = (m + n\sqrt{2})$

$\Rightarrow$ $(xy)z = (m + n\sqrt{2})(e + f\sqrt{2})$

$$= me + 2nf + (mf + ne)\sqrt{2}$$
$$= (ac + 2bd)e + 2(bc + ad)f + ((ac + 2ad)f + (bc + ad)e)\sqrt{2}$$
$$= (ac)e + (2bde) + 2(bc)f + 2(ad)f + ((ac)f + (2bd)f)\sqrt{2}$$
$$+ ((bc)e + ade)\sqrt{2}$$
$$= (ace + ceb\sqrt{2}) + 2df(a + b\sqrt{2}) + \sqrt{2}de(a + b\sqrt{2} + \sqrt{2}cf(a + b/2)$$
$$a(ke + 2fd) + \sqrt{2}(ed + cf)) + b\sqrt{2}(ce + 2fd + \sqrt{2}(de + c))$$
$$(a + b\sqrt{2})((ce + 2(d + \sqrt{2}(de + cf)]$$

which as simplification will give

$$= a(ce + ceb\sqrt{2}) + b(2ae + 2de\sqrt{2}) + 2b(ef\sqrt{2})$$
$$= (a + b\sqrt{2})((c + \sqrt{2d})(e + f\sqrt{2}))$$
$$= x(yz)$$

So S is associative under '$\cdot$'.

Commutative Property : S is commutative under '$\cdot$'.

For $xy = (a + b\sqrt{2})(c + d\sqrt{2})$

$$= (ac + 2bd) + (ad + bc)\sqrt{2}$$
$$= (ca + 2db) \neq (da + cb)\sqrt{2}$$
$$= (c + d\sqrt{2})(a + b\sqrt{2})$$
$$= yx$$

Existence of unity element. Since $1 \in I$ so $1 + 0\sqrt{2} \in S$

We claim $(a + b\sqrt{2})(1 + 0\sqrt{2}) = (a + b\sqrt{2}) = (1 + a\sqrt{2})(a + b\sqrt{2})$

To prove it since $(a + b\sqrt{2})(1 + a\sqrt{2}) = a + 2b0 + (a0 + b \cdot 1)\sqrt{2}$

$$= a + b\sqrt{2}$$
$$= (1 + 0\sqrt{2})(a + b\sqrt{2})$$

Hence $1 + 0\sqrt{2} \in S$ is Identity element of S.

Thus $(S, \cdot)$ is a commutative semigroup with unity element. Hence, So (ii) condition holds $(S, +, \cdot)$ is commutative ring with unity.

Lastly we show that S has no zero divisor. To prove it we must that $xy = 0 \Rightarrow x = 0$ or $y = 0$ NOTE

where $x = a + b\sqrt{2}\ y = a + d\sqrt{2}$

Non product we have

$$xy = (a + b\sqrt{2})(c + d\sqrt{2}) \quad \ldots(1)$$

$$= (ac + 2bd) + (ad + bc)\sqrt{2} \quad \ldots(2)$$

Now $xy = 0$

$$= (ac + 2bd) + (ad + bc)\sqrt{2} = 0 = 0 + 0\sqrt{2} \quad \ldots(3)$$

$\Rightarrow \quad ac + 2bd = 0 \quad \ldots(4) \quad$ and $\quad ad + bc = 0 \quad \ldots(5)$

Let us suppose $x \neq 0$ that $a + b\sqrt{2} = 0 \quad \Rightarrow \quad a \neq 0, b \neq 0.$

Solving these equations we can show that when $a \neq 0,\ b \neq 0$ then $c = 0$ and $d = 0$, similarly when $y \neq 0$ then $x = 0$. Thus $(S, +)$ is an integer domain. It is not a field since for any $(a + b\sqrt{2})$ its multiplication inverse x' will be such that $xx' = 1$

$$\Rightarrow x' = \frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{(a^2 - 2b^2)} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

But $\dfrac{a}{a^2 - 2b^2} \notin I$ and $-\dfrac{b}{a_1 - 2b_2} \notin I$ as they are not integers. So $x' \notin I$

Thus x can not have inverse in I under '$\cdot$'. So $(S, +, \cdot)$ can not be a field.

Example 7. If R is a ring and $a, b, c \in R$ the show *(i)* $-(a + b) = -a - b$ *(ii)* $a - (b + c) = (a - b) - c$

Solution. To prove (i) since $a, b \in R \Rightarrow -a, -b \in R$ and $(a + b) \in R$

Let us consider $(a + b) - a - b = a + b - a - b$

$= (a + (-a) + (b + (-b)$ Associative and commulative

$= 0 + 0$ Additive inverse property

$= 0$

$\Rightarrow -a - b$ is inverse of $(a + b)$ and so $-a - b = -(a + b)$

So (i) condition holds.

To prove (ii) let us consider $a - (b + c) = a - b - c$ from (i)

$= (a - b) - c$ Associative under +

Hence (ii) condition hold.

Example 8. Define ring. Give examples of the following.

(a) A commutative ring without unity element.

(b) A ring which is neither commutative nor having Identity element.

(c) Integral domain but not field.

Solution. For definition see 10.2.1.

(a) We have shown that set of even integer

$$I_2 = \{0, \pm 2, \pm 4, \pm 6, + \ldots\}$$

is commutative ring without identity element which can be easily varified.

(b) We have shown as example on matrices under division ring in 10.1.2. If we consider $M_{m \times n}[R] = \{A : A = (a_{ij})_{m \times n}\}$ as set of matrices of the form $m \times n$ with $a_{ij} \in R$ then

NOTE

$(M_{mn}(R), +)$ will always be an abelian group (see example1 of 8.3.1. (II) under group structure on matrices). We have also shown in the same section on example 2 on product of matrices that such matrices is associative but such matrices are neither commutative nor have identity element, because for Identity matrix, it must be square matrix. So such set of matrices will be non-commutative ring without Identity or unit element under addition and multiplication operation on matrices M_{mn}.

(c) We have already proved in example 4. The set of integer $(I, +, \cdot)$ is commutative ring with unity without zero derived, that is $(I, +, \cdot)$ is an integral domain but not field as it has no multiplication inverse.

Example 9. Prove the property (e) of ideal listed in theorem 10.7, that sum of two ideal is an ideal as defined in *(e)* containing each ideal.

Solution. let A, B be two ideals of ring $(R, +, \cdot)$ and the sum of $A + B$ is defined by

$$A + B = \{z : z = a + b \text{ where } a \in A \text{ and } b \in B\}$$

We claim (a) $A + B$ is an ideal

(b) $A \subseteq A + B$ and $B \subseteq A + B$

To prove (a) we must show that

(i) $(A + B)$ is a sub ring.

(ii) for $r \in R, z \in A + B \Rightarrow r \in A + B, zr \in A + B.$

To prove (i) Let $z_1, z_2 \in A + B$ be any pair of elements such that

$z_1 = a_1 + b_1$ and $z_2 = a_2 + b_2$ where $a_r, a \in A, b, b_1 \in R$

Then we must show that (1) $z_1 - z_2 \in A + B$ (2) $z_1 z_2 \in A + B$

Now to prove (1) we have $z_1 - z_2 = (a_1 + b_1) - (a_2 + b_2)$

$= a_1 + b_1 - a_2 - b_2$ proved $-(b + c) = -b - c$

$= (a_1 - a_2) + (b_1 - b_2)$ G-2 & G-5 condition under '+'

Now $a_1, a_2 \in A \Rightarrow a_1 - a_2 \in A$ and $b_1, b_2 \in B \Rightarrow b_1 - b_2 \in B$ as A and B are ideals so both are also subring. Therefore, $(a_1 - a) + (b - b_1) \in A + B$ by definition of $A + B$

$\Rightarrow z_1 - z_2 \in A + B$ So (i) condition holds

Now prove (2) let us consider $z_1 z_2 = (a_1 + b_1)(a_2 + b_2)$

$= (a_1 + b_1) a_2 + (a_1 + b_1) b_2$ Distributive property from left

$= a_1 a_2 + b_1 a_2 + a_1 b_2 + b_1 b_2$ Distributive property from right

Now A and B are A is closed under '$\cdot$' so for $a_1, a_2 \in A. a_1 a_2 \in A$ and $b_1, b_2 \in B \Rightarrow b_1 b_2 \in B$

Again $b_2 \in B$ and $B \subset R \Rightarrow b_2 \in R$

Now $a_1 \in A, b_2 \in R \Rightarrow a_1 b_2 \in A$ Since A is ideal

Similarly $b_1 \in B$ but $a_2 \in A \subset R \Rightarrow a_2 \in R$ so $b_1 a_2 \in B$ B being ideal

Thus we have $a_1 a_2 + a_1 b_2 \in A$, and $b_1 a_2 + b_1 b_2 \in B$

$\Rightarrow (a_1 a_2 + ab_1) + (b_1 a_1 + b_1 b_2) \in A + B \Rightarrow z_1 z_2 \in A + B$

Thus $(A + B)$ satisfies (1) and (2) so (i) condition of (a) holds, that is $(A + B)$ is a sub ring of $(R, +, \cdot)$

Again, to prove (ii) condition of (a) let $z \in A + B$ such that $z = a + b, a \in A, b \in B$ and $r \in R$ by any arbitrary element then we have to show that $rz \in A + B\ zr \in A + B$

Now $rz = r(a + b) = ra + rb$ Distributive property in R

Since both A and B are ideal so for $a \in A,\ r \in R \Rightarrow\ ra \in A$ and $b \in B\ r \in R \Rightarrow rb \in B$

$\Rightarrow$ $ra + rb \in A + B$ By definition of $(A + B)$

$\Rightarrow$ $rz \in A + B$ Similarly we can show $zr \in A + B$

So (ii) condition of (a) hold

From (1) and (II) of (a) it proves that $(A + B)$ is an ideal ring of R. Hence (a) condition holds.

To prove (b) that $A \subseteq A + B$ and $B \subseteq A + B$

Let $a \in A$ be any arbitrary element since $0 \in B$ as identity under '+'.

So $a = a + 0 \in A + B \Rightarrow a \in A + B$

Thus $a \in A \Rightarrow\ a \in A + B$

$\Rightarrow A \subseteq A + B$

Again to prove $B \subseteq A + B$

Let $b \in B$ be any arbitrary element then $b = 0 + b$ where $0 \in A, b \in B$

$\Rightarrow b = 0 + b\ \in A + B \Rightarrow b \in A + B$

Thus $b \in B \Rightarrow\ b \in A + B$

$\Rightarrow\ B \subseteq A + B$

So (b) condition holds.

Thus we show that sum of any two ideals is an ideal such each ideal is subset of sum of the ideals of ring R.

Example 10. If R be a commutative ring and $a \in R$ be any non-zero element of R then set. $Ra = \{ra : r \in R\}$ is an ideal of R.

Solution. This property gives us the condition how any ideal in any ring R can be generated that R must be commutative ring. Now to prove it let us consider the set $Ra = \{ra : r \in R\}$ for some arbitrary selected $a \in R$ then we will show that Ra is an ideal in R.

To have this condition we must show that

(a) Ra is sub ring of R.

(b) For any $x \in Ra$ and $x \in R \Rightarrow rx \in Ra$ and $xr \in Ra$

To prove (a) let $x, y \in Ra$ be any arbitrary elements such that $x = ra,\ y = sa$ for some $r, s \in R$ then we will show that (i) $x - y \in Ra$ (ii) $xy \in Ra$

Now to prove (i) we have $x - y = ra - sa$

$= (r - s)a$ Distributive property from left

Now $r, s \in R \Rightarrow\ r - s \in R \Rightarrow (r - s)a \in Ra$ By definition of Ra

$\Rightarrow\ x - y \in Ra$ So (i) condition holds.

To prove (ii) let us consider $xy = (ra)(sa)$,

Now $r \in R, a \in R \Rightarrow\ ra \in R$ Let $p = ra \in R$ then we have

$xy = (ra)(sa) = p(sa) = (ps)a\ \ p \in R\ s \in R \Rightarrow ps \in R$

$\Rightarrow (ps)a \in Ra$ By definition of Ra

$\Rightarrow xy \in Ra$

Hence (ii) condition holds. Thus Ra satisfies (i) and (ii) so Ra must be subring of R.

Now to prove (b) let $x \in Ra$ be such that $x = sa$ for some $s \in R$

then we have $rx \equiv r(sa) = (rs)a$

Now $r, s \in R \Rightarrow\ rs \in R \Rightarrow (rs)a \in Ra$ By definition of Ra

$\Rightarrow\ rx \in Ra$

Again let us consider $xr = (sa)r = s(ar)$ By Associative Condition

NOTE

NOTE

$= s(ra)$ — R is commutative $a \in R, r \in R$

$= (sr)a$ — By Associative Condition

Now as $sr \in R \Rightarrow (sr)a \in Ra \Rightarrow xr \in Ra$

Thus we have $rx \in Ra$ and $xr \in Ra$ for any $x \in Ra$ and $r \in R$

So (b) condition holds thus (a) and (b) condition hold. So Ra must be an ideal of R.

Supplementary Examples

1. Prove the following is any ring $(R, +)$ let $a, b, c, d \in a$ then

(i) $(a+b)(c+d) = ac + ad + bc + bd$

(ii) $(a-b)(c-d) = (ac+bd) - (ad+bc)$

(iii) $(a-b)^2 = a^2 - ab - ba + b^2$

(iv) If $(R, +)$ commutative then $(a+b)^2 = a^2 + 2ab + b^2$

(v) $(a-b)(a+b) = a^2 + ab - ba - b^2$

Show that when R is commutative then it becomes $(a^2 - b^2)$

2. Show that set of integer I becomes a ring under two binary operator 'o' and '$*$' defined by

(i) $aob = a + b + 1$ and

(ii) $a * b = ab + a + b$

what is identity element for 'o' and for '$*$' if exists?

3. Show that $M_2(z)$ - the set of all matrices of 2×2 expressed as

$M_2(Z) = \left\{ \begin{bmatrix} x & x \\ -x & x \end{bmatrix} : x, y \in Z \right\}$ where Z denotes the set integers,

is a commutative ring with respect to matrix addition and multiplication.

Does it have divisor of zero? (ii) Does it have unity element?

4. Let $(R, +, \cdot)$ be Boolean ring, such that $a^2 = a \ \forall a \in R$. Then show that $2a = 0 \forall \ a \in R$ and duduce that Boolean ring is commutative.

5. Prove that Skew field (Divisor Ring) $(S, +, \cdot)$ satisfies the following :

(i) It contains no divisor of zero.

(ii) The non-zero elements of it forms a group under '$\cdot$….

6. In an integral domain $(D, +, \cdot)$ then show that if $ba = ac$ with $a \neq 0$ then $b = c$.

7. Show that under modulo 6 proved as commutative ring with unity under examples (ii) in 10.2.2. the following subsets are its ideals.

(i) $S = \{[0], [2], [4]\}$

(ii) $S = \{[0], [3]\}$

8. Prove the properties of an ideals listed in (a), (b), (c) in theorem 10.7.

9. Show that the following properties for any $a, b \in F$ hold for any field $(F, +, \cdot)$.

(i) $(-a)(b) = -(ab)$

(ii) $(-a)(-b)^{-1} = (ab^{-1})$

(iii) $(a^{-1})^{-1} = a$

10. Prime the properties listed in (a) and (b) as Homomorphism of ring in theorem 10.8.3.